

# Data updating method and data updating system

Publication number: JP2003337923 (A)

Publication date: 2003-11-28

Inventor(s):

Applicant(s):

Classification:

- International: G06F12/14; G06F21/00; G06F21/20; G06F21/24; G06K17/00; G07F7/10; G06F12/14; G06F21/00; G06F21/20; G06K17/00; G07F7/10; (IPC1-7): G06K17/00; G06F12/14; G06F15/00

- European: G06F21/00N5A; G07F7/10D4E2

Application number: JP20020144486 20020520

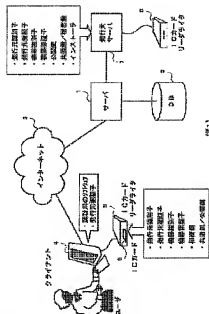
Priority number(s): JP20020144486 20020520

Also published as:

JP3754004 (B2)  
EP1365307 (A2)  
EP1365307 (A3)  
EP1365307 (B1)  
US2003217270 (A1)

Abstract of JP 2003337923 (A)

PROBLEM TO BE SOLVED: To provide a method and a system for data update which can update data of an IC card through a network without mistaking the IC card to be updated.



Data supplied from the esp@cenet database — Worldwide



## 【特許請求の範囲】

【請求項1】 機器認証に用いる秘密鍵を記憶する装置についてサーバが機器認証を行い、当該秘密鍵に対応する公開鍵を用いて暗号化された更新データを前記装置が接続するクライアントに送信し、当該クライアントが前記装置に当該更新データを入力し、前記装置が前記秘密鍵で前記更新データを復号し、復号した更新データで装置内のデータ更新を行うことを特徴とするデータ更新方法。

【請求項2】 機器認証に用いる秘密鍵を記憶する装置についてサーバが機器認証を行い、当該秘密鍵に対応する公開鍵を用いて暗号化された更新データを前記装置が接続するクライアントに送信し、当該クライアントが前記装置に当該更新データを入力し、前記装置が前記更新データを記憶し、更新データが利用される毎に前記秘密鍵で前記更新データを復号し、復号した更新データを利用のために提供することを特徴とするデータ更新方法。

【請求項3】 機器認証に用いる秘密鍵を記憶する装置には、共通鍵又は公開鍵で暗号化された発行元認証子が記憶され、サーバは前記共通鍵又は前記公開鍵に対応する秘密鍵を用い、前記装置からの暗号化された発行元機器認証子を当該共通鍵又は当該秘密鍵で復号して発行元識別子を取得し、当該取得した発行元識別子と記憶する発行元識別子とを比較照合して発行元サーバ認証を行うことを特徴とする請求項1又は2記載のデータ更新方法。

【請求項4】 クライアントは、発行元から発行元認証子を取得し、発行元サーバ認証の前に、装置から読み込んだ発行元認証子と前記取得した発行元認証子とを比較照合して発行元クライアント認証を行うことを特徴とする請求項3記載のデータ更新方法。

【請求項5】 装置は、本人認証の機能を備え、発行元クライアント認証、本人認証、発行元サーバ認証、機器認証を行い、データ更新を行うことを特徴とする請求項4記載のデータ更新方法。

【請求項6】 機器認証に用いる秘密鍵を記憶する装置と、機器認証が為されると、前記秘密鍵に対応する公開鍵で暗号化された更新データを機器認証が為された装置宛に送信するサーバと、

前記送信された暗号化された更新データを受信して前記装置に出力するクライアントとを備え、

前記装置は、前記クライアントから入力された暗号化された更新データを前記秘密鍵で復号し、当該復号した更新データで装置内のデータ更新を行う装置であることを特徴とするデータ更新システム。

【請求項7】 機器認証に用いる秘密鍵を記憶する装置と、機器認証が為されると、前記秘密鍵に対応する公開鍵で暗号化された更新データを機器認証が為された装置宛に

送信するサーバと、前記送信された暗号化された更新データを受信して前記装置に出力するクライアントとを備え、

前記装置は、前記クライアントから入力された暗号化された更新データを記憶し、更新データが利用される毎に前記秘密鍵で前記更新データを復号し、当該復号した更新データを利用のために提供する装置であることを特徴とするデータ更新システム。

【請求項8】 サーバは、乱数を発生させ、当該乱数をクライアントに送信すると共に、前記クライアントから受信した暗号化された乱数を受信した機器識別子に対応する公開鍵で復号し、当該復号された乱数と前記発生させた乱数を比較照合して機器認証を行うサーバであり、前記クライアントは、前記サーバから受信した乱数を装置に出力すると共に、前記装置から入力された暗号化された乱数及び機器識別子を前記サーバに送信するクライアントであり、

前記装置は、前記クライアントから入力された乱数を前記秘密鍵で暗号化し、記憶する機器識別子と前記暗号化された乱数を前記クライアントに出力する装置であることを特徴とする請求項6又は7記載のデータ更新システム。

【請求項9】 サーバは、乱数と、機器識別子を暗号化するための共通鍵をクライアントに送信し、前記クライアントから受信した暗号化された機器識別子を前記共通鍵で復号し、当該復号された機器識別子に対応する公開鍵で暗号化された乱数を復号し、当該復号された乱数と前記発生させた乱数を比較照合して機器認証を行うサーバであり、

前記クライアントは、前記サーバから受信した乱数及び共通鍵を装置に出力すると共に、前記装置から入力された暗号化された乱数及び暗号化された機器識別子を前記サーバに送信するクライアントであり、

前記装置は、前記クライアントから入力された乱数を前記秘密鍵で暗号化し、記憶する機器識別子を前記共通鍵で暗号化し、前記暗号化された乱数及び前記暗号化された機器識別子を前記クライアントに出力する装置であることを特徴とする請求項8記載のデータ更新システム。

【請求項10】 装置は、秘密鍵で暗号化された機器認証子をクライアントに出力する装置であり、

前記クライアントは、前記装置から入力された機器認証子をサーバに送信するクライアントであり、

前記サーバは、前記クライアントから受信した機器認証子を当該機器認証子に対応する公開鍵で復号して機器識別子を取得し、当該取得した機器識別子と記憶する機器識別子とを比較照合して機器認証を行うサーバであることを特徴とする請求項6又は7記載のデータ更新システム。

【請求項11】 サーバとクライアント間の通信パケットが暗号化されることを特徴とする請求項8乃至10の

いずれか記載のデータ更新システム。

【請求項 12】 装置は、発行元認証に用いる共通鍵又は公開鍵を記憶し、当該共通鍵又は公開鍵で暗号化された発行元認証子をクライアントに出力する装置であり、前記クライアントは、前記暗号化された発行元認証子をサーバに送信するクライアントであり、前記サーバは、発行元認証に用いる共通鍵又は秘密鍵を記憶し、前記クライアントから受信した暗号化された発行元機器認証子を当該記憶する共通鍵又は秘密鍵で復号して発行元識別子を取得し、当該取得した発行元識別子と記憶する発行元識別子とを比較照合して発行元サーバ認証を行うサーバであることを特徴とする請求項 8 乃至 11 のいずれかに記載のデータ更新システム。

【請求項 13】 クライアントは、発行元から発行元認証子を取得し、発行元サーバ認証の前に、装置から読み込んだ発行元認証子と前記取得した発行元認証子とを比較照合して発行元クライアント認証を行うクライアントであることを特徴とする請求項 12 記載のデータ更新システム。

【請求項 14】 装置は、本人認証の機能を備え、クライアントでは発行元クライアント認証を、前記装置では本人認証を、サーバでは発行元サーバ認証、機器認証を、前記装置ではデータ更新を行うことを特徴とする請求項 13 記載のデータ更新システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、ICカード等に記憶されているデータを、ネットワークを介して新規登録や追加登録を含む更新を行うデータ更新方法に係り、特に、装置を間違えなく特定して更新することができ、確実、安全に人手を介さずに更新できるデータ更新方法及びデータ更新システムに関する。

【0002】

【従来の技術】従来、ICカード（スマートカード）その他取り外し可能な本人認証の機能を備えた装置に記憶された重要なデータ、例えば、ネットワークパスワード、電子証明書、シングルサインオンするための情報の追加、ダイヤルアップ情報、ICカード/スマートカードや指紋照合トークン内情報、有効期限等の重要な情報を更新する場合には、当該ICカードを一旦回収してデータの書き換えを行って本人に戻すか、そのカードを無効にして更新データが書き込まれた新規のカードを本人に発行するかのいずれかの方法が採用されている。

【0003】尚、個人認証に用いる重要データを更新する技術ではないが、個人認証に関する従来技術には、平成14年3月12日公開の特開2002-73571「個人認証システムおよび個人認証方法、並びにプログラム提供媒体」（出願人：ソニー株式会社、発明者：渡辺秀明他）がある。この発明は、個人識別データであるテンプレートを格納した個人識別証明書を用いた個人認

証システムにおける個人識別証明書の管理を行うものである。

【0004】

【発明が解決しようとする課題】しかしながら、上記従来の取り外し可能な本人認証機能を備えた装置内部のデータ更新方法では、回収・再発行又は新規発行の手間が掛かり、重要データが外部に漏洩することなくネットワークを介して更新できず、利便性に欠けるという問題点があった。

【0005】本発明は上記実情に鑑みて為されたものであり、装置を間違えなく特定し、ネットワークを介して記録媒体のデータを新規登録や追加登録を含む更新を自動で又は処理を起動して行うことができるデータ更新方法及びデータ更新システムを提供することを目的とする。

【0006】

【課題を解決するための手段】本発明は、新規登録又は追加登録を含む更新を行うデータ更新方法において、機器認証に用いる秘密鍵を記憶する装置についてサーバが機器認証を行い、当該秘密鍵に対応する公開鍵を用いて暗号化された更新データを装置が接続するクライアントに送信し、当該クライアントが装置に当該更新データを入力し、装置が秘密鍵で更新データを復号し、復号した更新データで装置内のデータ更新を行うものであり、更新データを書き替える対象の装置を間違えることなく、機器認証に用いる秘密鍵を保有する装置のみが更新データを復号して更新でき、更新データの秘匿性を保持し、ネットワークを介して装置内のデータ更新を実現できる。

【0007】本発明は、新規登録又は追加登録を含む更新を行うデータ更新方法において、機器認証に用いる秘密鍵を記憶する装置についてサーバが機器認証を行い、当該秘密鍵に対応する公開鍵を用いて暗号化された更新データを装置が接続するクライアントに送信し、当該クライアントが装置に当該更新データを入力し、装置が更新データを記憶し、更新データが利用される毎に秘密鍵で更新データを復号し、復号した更新データを利用のために提供するものであり、更新データの記憶先となる装置を間違えることなく、機器認証に用いる秘密鍵を保有する装置のみが更新データを復号して利用でき、更新データの秘匿性を保持し、ネットワークを介して装置内のデータ提供を実現できる。

【0008】本発明は、データ更新システムにおいて、機器認証に用いる秘密鍵を記憶する装置と、機器認証が為されると、秘密鍵に対応する公開鍵で暗号化された更新データを機器認証が為された装置宛に送信するサーバと、送信された暗号化された更新データを受信して装置に出力するクライアントとを備え、装置は、クライアントから入力された暗号化された更新データを秘密鍵で復号し、当該復号した更新データで装置内のデータ更新を

行装置としており、更新データを書き替える対象の装置を間違えることなく、機器認証に用いる秘密鍵を保有する装置のみが更新データを復号して更新でき、更新データの秘匿性を保持し、ネットワークを介して装置内のデータ更新を実現できる。

【0009】本発明は、データ更新システムにおいて、機器認証に用いる秘密鍵を記憶する装置と、機器認証が為されると、秘密鍵に対応する公開鍵で暗号化された更新データを機器認証が為された装置宛に送信するサーバと、送信された暗号化された更新データを受信して装置10 に出力するクライアントとを備え、装置は、クライアントから入力された暗号化された更新データを記憶し、更新データが利用される毎に秘密鍵で更新データを復号し、当該復号した更新データを利用のために提供する装置としており、更新データの記憶先となる装置を間違えることなく、機器認証に用いる秘密鍵を保有する装置のみが更新データを復号して利用でき、更新データの秘匿性を保持し、ネットワークを介して装置内のデータ提供を実現できる。

【0010】本発明は、上記データ更新方法又は上記データ更新システムにおいて、発行元クライアント認証、本人認証、発行元サーバ認証を行うものであり、セキュリティを向上させることができる。

【0011】

【発明の実施の形態】本発明の実施の形態について図面を参照しながら説明する。本発明の実施の形態に係るデータ更新システムは、本人認証、発行元認証、機器認証の各認証が為されると、機器認証に対応する公開鍵で暗号化された更新データをサーバがクライアントに送信すると、ICカードが当該暗号化された更新データをICカード内の機器認証子に対応する秘密鍵で復号化し、その復号した更新データでICカード内の書き換えを行うものである。これにより、ICカードを回収することなく、重要データの秘匿性を保持しつつネットワークを介してICカード内の重要データの更新（新規登録又は追加登録を含む）を自動で又は処理を起動して行うことができるものである。

【0012】本発明の実施の形態に係るデータ更新システム（本システム）について図1を参照しながら説明する。図1は、本発明の実施の形態に係るデータ更新システムの概略構成図である。本システムは、図1に示すように、サーバ1と、DB（データベース）2と、インターネット3と、クライアント4と、ICカードリーダーライタ5と、ICカード6と、発行元サーバ7と、ICカードリーダーライタ8とから基本的に構成されている。図1では、説明を簡単にするために、クライアント4、ICカードリーダーライタ5、ICカード6は一台づつしか描画していないが、インターネット3に接続するクライアント4等は複数あるものである。また、クライアント4とサーバ1は、インターネット3を介して接続され、

発行元サーバ7はサーバ1に接続している。

【0013】次に、本システムの各部を具体的に説明する。サーバ1は、クライアント4からのインターネット3を介しての本処理（更新処理）に際しては、本人認証処理、発行元認証処理、機器認証処理を行い、全て認証されると、DB2に記憶するクライアントに関するデータ（暗号データ）を、インターネット3を介してクライアント4に送信する。

【0014】ここで、本人認証処理は、指紋データ、音声データ、顔の画像データ、又は瞳孔、網膜、サイン、掌形の画像データ等の生体データ及び/又はPIN（Personal Identification Number）を用いた単独又は複合認証であり、ICカード6とクライアント4との間で、若しくはICカード6内で認証を行う。

【0015】また、発行元認証処理は、クライアント4が保持する認証用のソフトウェア（インストーラによってインストールされたソフトウェア）の動作により、ICカード6内の発行元認証子とクライアント4のメモリ内の発行元認証子とを比較照合して認証を行う発行元クライアント認証と、認証用のソフトウェアの動作により、ICカード6内の発行元認証子をサーバ1に送信し、サーバ1で送信された発行元認証子を復号して発行元識別子を取得し、その発行元識別子とDB2に記憶する発行元識別子とを比較照合して認証を行う発行元サーバ認証とを有する。インストーラは、発行元サーバ7からオンライン又はオフラインにてクライアント4に提供されるものである。

【0016】特に、発行元サーバ認証を具体的に説明すると、ICカード6の発行元が付与した発行元識別子とそれを共通鍵又は公開鍵（共通鍵/公開鍵）で暗号化した発行元認証子がICカード6に記憶されており、その暗号化された発行元認証子がICカード6からクライアント4を介してサーバ1に送信され、サーバ1で暗号化された発行元認証子を共通鍵又は秘密鍵（共通鍵/秘密鍵）で復号して発行元識別子を取り出し、DB2に記憶する発行元識別子と比較して復号した発行元識別子が適正であるか否かを判断する。ここで、発行元認証子における暗号化及び復号化に用いる暗号鍵方式は、共通鍵方式又は公開鍵方式を用いている。特に、公開鍵方式の場合、公開鍵を保有するのはICカード6側であり、また、サーバ1には、接続する発行元サーバ7からICカード6に発行した発行元識別子と発行元認証子が予め提供されており、その発行元識別子と発行元認証子はDB2に記憶される。

【0017】更に、機器認証処理は、チャレンジレスポンス（オンライン認証）を用いた機器認証である。具体的には、サーバ1で乱数を生産させ、その乱数をクライアント4に送信する。クライアント4は、サーバ1から受信した乱数をICカード6に出力し、ICカード6は

保有する秘密鍵でその乱数を暗号化し、その暗号化した乱数及び保有する機器識別子をクライアント4に出力して、クライアント4が暗号化した乱数及び機器識別子をサーバ1に送信する。すると、サーバ1は、機器識別子から対応する公開鍵を取得し、暗号化された乱数をその公開鍵で復号化し、復号した乱数を発生させた乱数と比較照合し、一致すれば機器認証が成功したとする。

【0018】また、サーバ1が、ICカード6における機器識別子を暗号化するための共通鍵を乱数と共に送信してもよい。この場合、ICカード6では、受信した共通鍵を用いて機器識別子を暗号化し、暗号化した乱数と暗号化した機器識別子をサーバ1に送信する。そして、サーバ1は、受信した暗号化された機器識別子を内部に保持する共通鍵で復号し、復号した機器識別子に対応する公開鍵を取得し、その公開鍵で暗号化された乱数を復号化して乱数の比較照合を行う。

【0019】また、サーバ1とクライアント4との間における通信パケットをSSL (Secure Socket Layer) 又はVPN (Virtual Private Network) 等の技術を用いて暗号化してもよい。SSL等の暗号化はサーバ1とクライアント4との間で有効であるが、クライアント4とICカード6との間については、本処理が機密保護について有効である。

【0020】尚、チャレンジレスポンスを用いない機器認証の場合には、ICカード6が記憶する機器識別子を、記憶する秘密鍵で暗号化して機器認証子を生成し、クライアント4に出力する。クライアント4は、暗号化された機器認証子をサーバ1に送信し、サーバ1が暗号化された機器認証子に対応する公開鍵で復号して機器識別子を取得し、その機器識別子とDB2に記憶する機器識別子と比較照合し、一致すれば機器認証が成功したものとすもよい。

【0021】また、サーバ1は、ICカード6内の重要データを更新するための更新データを暗号化してDB2に記憶している。その暗号化方法は、機器識別子に対応する公開鍵を用いて暗号化している。そして、サーバ1は、ICカード6内の重要データを更新するために、DB2に記憶する暗号化された更新データを、インターネット3を介してクライアント4に送信する。

【0022】DB (データベース) 2は、発行元認証を行うための発行元識別子、発行元認証子、共通鍵/秘密鍵、機器認証を行うための機器識別子、機器認証子、公開鍵、ICカード6の重要データを更新するための暗号化された更新データを記憶している。ここで、発行元識別子を暗号化したのが発行元認証子で、乱数又は機器識別子を暗号化したのが機器認証子である。尚、サーバ1での認証処理では、復号された発行元識別子、機器識別子が取得されるので、DB2には、発行元認証のための発行元識別子、共通鍵/秘密鍵、機器認証のための機器識別子、公開鍵、更新データを最小限記憶していれば足

りる。

【0023】インターネット3は、サーバ1とクライアント4との間の通信媒体である。インターネット3の代わりにWAN (Wide Area Network) 又はLAN (Local Area Network) 等の通信媒体であってもよい。

【0024】クライアント4は、本システムに接続するコンピュータであり、本人認証、発行元認証、機器認証等の認証により本システムにおける更新処理が許可され、サーバ1からの情報をICカード6に書き込む。尚、クライアント4には発行元サーバ7がネットワークを介したオンラインで又はCD-ROM等の記録媒体を介したオフラインで発行されたインストールによってインストールされた認証用のソフトウェアを保持しており、クライアントにおける発行元認証 (発行元クライアント認証) を行うと共に、サーバ1にICカード6内の発行元認証子を送信してサーバにおける発行元認証 (発行元サーバ認証) を行う。

【0025】具体的には、クライアント4は、認証用のソフトウェアを動作させ、発行元クライアント認証を行うために、ICカード6からICカードリーダーライタ5で発行元認証子を読み込み、メモリに記憶する発行元認証子と比較照合し、一致すれば発行元クライアント認証が成功したのとして、次に発行元サーバ認証を行う。クライアント4は、発行元サーバ認証のために、ICカード6からICカードリーダーライタ5で発行元認証子を読み取ってインターネット3を介してサーバ1に送信する。

【0026】また、クライアント4は、機器認証のために、サーバ1から受信した乱数をICカード6に出力し、ICカード6において機器識別子に対応する秘密鍵でその乱数を暗号化して生成された機器認証子と、それに加えて機器識別子をICカード6からICカードリーダーライタ5で読み取り、インターネット3を介してその機器認証子及び機器識別子をサーバ1に送信する。そして、各認証が為されると、データの更新処理として、クライアント4は、サーバ1から暗号化された更新データを受信し、そのデータをICカード6に出力する。また、クライアント4は、ネットワークに接続可能なパーソナルコンピュータ (PC)、個人情報端末 (PD

A)、携帯電話、PHS、情報家電であってもよい。【0027】本人認証は、生体データ、PINデータを単独又は複合的に用いて行われるもので、ICカード6内又はICカード6とクライアント4との間で認証される。また、暗号化された発行元認証子と機器認証子もICカード6から読み込まれてクライアント4からサーバ1に送信される。ここで、本人認証で本人と認められない場合には、それに続く発行元認証、機器認証を行わない。

【0028】ICカードリーダーライタ5は、ICカード6内の情報を読み取ってクライアント4に出力し、ま

た、クライアント4からの指示によりICカード6に情報を書き込む処理を行う。

【0029】ICカード6は、CPU (Central Processing Unit) を備えて独立して処理を行うことができるものであり、本人認証を行う生体データ、PINデータを、発行元認証を行うための発行元識別子、発行元認証子、共通鍵/公開鍵を、機器認証を行うための機器識別子、秘密鍵を記憶している。ここで、各データは、ICカード6を無理にこじ開けた場合に、消滅する耐タンパ性を備えている。

【0030】ICカード6は、内部に保持する生体データ、PINデータによって本人認証を行い、発行元クライアント認証においては発行元認証子をクライアント4に出力し、また、発行元サーバ認証においては発行元認証子をクライアント4に出力する。そして、チャレンジレスポンスによる機器認証の場合、ICカード6は、サーバ1から送信された乱数をクライアント4から入力し、その乱数を秘密鍵で暗号化して機器認証子を生成し、生成した機器認証子と機器識別子をクライアント4に出力する。機器認証子及び機器識別子は、クライアント4からサーバ1に送信される。

【0031】また、サーバ1から、ICカード6における機器識別子を暗号化するための共通鍵を乱数と共に送信してもよい。この場合、ICカード6は、受信した共通鍵を用いて機器識別子を暗号化し、暗号化した乱数と暗号化した機器識別子をサーバ1に送信する。そして、サーバ1は、受信した暗号化された機器識別子を内部に保持する共通鍵で復号し、復号した機器識別子に対応する公開鍵を取得し、その公開鍵で暗号化された乱数を復号化して乱数の比較照合を行う。これにより、暗号化されていない機器識別子がネットワークを流れることを防止できる。また、サーバ1とクライアント4との間における通信パケットをSSL又はVPN等の技術を用いて暗号化してもよい。

【0032】また、チャレンジレスポンスによらない機器認証の場合、ICカード6は、機器識別子を秘密鍵で暗号化して機器認証子を生成し、その機器認証子をクライアント4に出力する。

【0033】尚、本システムでは、ICカードを例に説明したが、トークン、独立型指紋認証装置 (IAU: Intelligent Authentication Unit)、その他取り外し可能な本人認証機能を備えた装置であってもよい。

【0034】発行元サーバ7は、ICカードリーダライタ8を備え、ICカード6の発行元で決められた発行元認証のための発行元識別子、発行元認証子、共通鍵/公開鍵及びICカード6の各々に対応した機器認証のための機器識別子、機器認証子、秘密鍵をICカード6にオフラインで書き込むと共に、サーバ1に当該ICカード6の発行元識別子、発行元認証子、共通鍵/秘密鍵と機器識別子、機器認証子、公開鍵をオンラインで送信し、

DB2に発行元認証子、機器認証子等を記憶する。ここで、発行元識別子、発行元認証子は発行元にユニークな情報であり、機器識別子、機器認証子は機器にユニークな情報である。また、発行元サーバ7は、クライアント4の認証用のソフトウェアの動作によって発行元クライアント認証のための発行元認証子をクライアント4に登録する。

【0035】発行元認証のためにICカード6に書き込まれる共通鍵/公開鍵とDB2に書き込まれる共通鍵/秘密鍵は対応しており、また、機器認証のためにICカード6に書き込まれる秘密鍵とDB2に書き込まれる公開鍵は対応しており、一方の鍵で暗号化されたデータを他方の鍵で復号できるものとなっている。尚、機器認証のためのDB2に書き込まれる公開鍵は、ICカード6で更新される更新データを暗号化するのに用いられ、機器認証のためのICカード6に書き込まれる秘密鍵は、サーバ1から送信される暗号化された更新データを復号するのにも用いられる。

【0036】尚、チャレンジレスポンスによる機器認証を行う場合は、ICカード6に書き込む機器認証のための情報は、機器識別子と秘密鍵である。チャレンジレスポンスによらない機器認証を行う場合は、ICカード6に書き込む機器認証のための情報は、機器識別子、機器認証子、秘密鍵である。ここで、機器認証のために、機器識別子を秘密鍵で暗号化して機器認証子を生成してサーバ1に送信すれば、ICカード6には機器識別子と秘密鍵が書き込まれればよい。

【0037】次に、本システムの動作について図2、図3、図4を用いて説明する。図2は、本発明の実施の形態に係る新規登録又は追加登録を含む更新処理を行うデータ更新システムにおける処理の概要を示す処理概略図であり、図3は、サーバ1における処理の流れを示すフローチャートであり、図4は、ICカード6における処理の流れを示すフローチャートである。

【0038】図2に示すように、クライアント4は、認証用ソフトウェアが動作し、ICカード6から発行元認証子を読み込み、クライアント4内の発行元認証子と比較照合して発行元クライアント認証(1)を行う。比較照合の結果、一致していれば発行元クライアント認証が成功したとして、次に、ユーザは生体データ又はPINデータ等を用いてICカード6での本人認証(2)を行う。

【0039】本人認証が適正であれば、次に、ICカード6は、発行元認証子をクライアント4からサーバ1に送信してサーバ1での発行元サーバ認証(3)を行う(S1)。発行元サーバ認証は、ICカード6から出力された発行元認証子をサーバ1が受信し、DB2に記憶する復号のための共通鍵/秘密鍵を用いて復号化し、復号された発行元識別子を取得して、DB2に記憶する発行元識別子と比較照合する。比較照合結果、一致すれば

発行元サーバ認証が成功したとして、次に機器認証(4)を行う。

【0040】チャレンジレスポンスによる機器認証(4)(S2)は、サーバ1で乱数を生じさせ、クライアント4を介してICカード6にその乱数を送信する。ICカード6では機器認証のための秘密鍵でその乱数を暗号化し、機器識別子(又はサーバ1から送信された共通鍵で暗号化された機器識別子)と暗号化された乱数をクライアント4を介してサーバ1に送信する。サーバ1は、機器識別子(暗号化された機器識別子であればサーバ1が保持する共通鍵で復号した機器識別子)に対応する公開鍵で暗号化された乱数を復号し、復号した乱数と当初発生させた乱数と比較照合して、機器認証を行う。比較照合の結果、両者が一致すれば、機器認証は成功したものとなる。

【0041】また、チャレンジレスポンスによらない機器認証の場合、ICカード6は機器識別子を機器認証のための秘密鍵で暗号化して機器認証子を生じ、クライアント4を介してサーバ1に送信する。サーバ1は、機器認証子を受信し、その機器認証子に対応する公開鍵で機器認証子を復号して機器識別子を取得し、DB2に記憶する機器識別子と復号した機器識別子とを比較照合して、機器認証を行う。比較照合の結果、両者が一致すれば、機器認証は成功したものとなる。

【0042】機器認証が適正に終了すると、サーバ1は、機器認証のための公開鍵で暗号化された更新データをDB2から読み込み、クライアント4にインターネット3を介して転送し、クライアント4はその暗号化された更新データをICカード6に出力する(5)(S3)。

【0043】更に、ICカード6は、暗号化された更新データを入力し(S11)、当該更新データをICカード内の機器認証のための秘密鍵で復号化する(S12)(6)。そして、復号化された復号データでICカード6内の重要なデータを書き替えて更新する(S13)(7)。尚、ICカード6は、入力した暗号化された更新データをそのままの状態で記憶し、当該更新データを参照する必要が発生した場合に秘密鍵で復号して利用するようにしてもよい。

【0044】本システムによれば、本人認証、発行元認証、機器認証を行い、機器認証のための公開鍵で暗号化された更新データをサーバ1がDB2から読み取ってクライアント4に送信し、クライアント4では受信した暗号化された更新データをICカード6に出力し、ICカード6は、機器認証のための秘密鍵で更新データを復号して、ICカード6内のデータの書き換えを行うようにしているので、機器認証を行うことで更新データを書き替える対象のICカードを間違えることなく、更新データが盗聴されたとしても、機器認証のための秘密鍵を保有するICカード6のみがデータを復号可能であるた

めセキュリティを向上させることができ、サーバ1は対象とするICカード6内の重要なデータを、ネットワークを介して更新できる効果がある。

【0045】また、本システムでは、ICカード6内のデータ更新の処理について説明したが、ユーザが本システムのネットワークにログインする際に、本人認証、発行元認証、機器認証を行い、ユーザが意識した処理をすることなく、自動でシステム変更に伴うデータをICカード6に書き込むことが可能となる。これにより、アプリケーションの有効期限、更新期限、電子証明書の有効期限の更新、ネットワークパスワードのユーザ毎の定期的変更等を容易に行うことができる効果がある。

【0046】具体的には、ネットワークパスワードを定期的に更新する場合は、変更日にDB2に変更されたパスワードを公開鍵で暗号化してセットし、ユーザログインにより、各認証が行われ、適正であればサーバ1がDB2から暗号化されたパスワードをクライアント4に送信し、クライアント4が暗号化されたパスワードをICカード6に出力する。ICカード6は、入力された暗号化されたパスワードを秘密鍵で復号し、その復号したパスワードをICカード6内に記憶する。これにより、ICカード6におけるネットワークパスワードが変更されたことになる。

【0047】

【発明の効果】本発明によれば、機器認証に用いる秘密鍵を記憶する装置についてサーバが機器認証を行い、当該秘密鍵に対応する公開鍵を用いて暗号化された更新データを装置が接続するクライアントに送信し、当該クライアントが装置に当該更新データを入力し、装置が秘密鍵で更新データを復号し、復号した更新データで装置内のデータ更新を行う、新規登録又は追加登録を含む更新を行うデータ更新方法としているので、更新データを書き替える対象の装置を間違えることなく、機器認証に用いる秘密鍵を保有する装置のみが更新データを復号して更新でき、更新データの秘匿性を保持し、ネットワークを介して装置内のデータ更新を実現できる効果がある。

【0048】本発明によれば、機器認証に用いる秘密鍵を記憶する装置についてサーバが機器認証を行い、当該秘密鍵に対応する公開鍵を用いて暗号化された更新データを装置が接続するクライアントに送信し、当該クライアントが装置に当該更新データを入力し、装置が更新データを記憶し、更新データが利用される毎に秘密鍵で更新データを復号し、復号した更新データを利用するために提供する、新規登録又は追加登録を含む更新を行うデータ更新方法としているので、更新データの記憶先となる装置を間違えることなく、機器認証に用いる秘密鍵を保有する装置のみが更新データを復号して利用でき、更新データの秘匿性を保持し、ネットワークを介して装置内のデータ提供を実現できる効果がある。

【0049】本発明によれば、機器認証に用いる秘密鍵



を記憶する装置と、機器認証が為されると、秘密鍵に対応する公開鍵で暗号化された更新データを機器認証が為された装置宛に送信するサーバと、送信された暗号化された更新データを受信して装置に出力するクライアントとを備え、装置は、クライアントから入力された暗号化された更新データを秘密鍵で復号し、当該復号した更新データで装置内のデータ更新を行うデータ更新システムとしているので、更新データを書き替える対象の装置を間違えることなく、機器認証に用いる秘密鍵を保有する装置のみが更新データを復号して更新でき、更新データの秘匿性を保持し、ネットワークを介して装置内のデータ更新を実現できる効果がある。

【0050】本発明によれば、機器認証に用いる秘密鍵を記憶する装置と、機器認証が為されると、秘密鍵に対応する公開鍵で暗号化された更新データを機器認証が為された装置宛に送信するサーバと、送信された暗号化された更新データを受信して装置に出力するクライアントとを備え、装置は、クライアントから入力された暗号化された更新データを記憶し、更新データが利用される毎に秘密鍵で更新データを復号し、当該復号した更新データを利用のために提供するデータ更新システムとしているので、更新データの記憶先となる装置を間違えることなく、機器認証に用いる秘密鍵を保有する装置のみが更

\* 新データを復号して利用でき、更新データの秘匿性を保持し、ネットワークを介して装置内のデータ提供を実現できる効果がある。

【0051】本発明によれば、発行元クライアント認証、本人認証、発行元サーバ認証を行う上記データ更新方法又は上記データ更新システムとしているので、セキュリティを向上させることができる効果がある。

【図面の簡単な説明】

【図1】本発明の実施の形態に係るデータ更新システムの概略構成図である。

【図2】本発明の実施の形態に係る新規登録又は追加登録を含む更新処理を行うデータ更新システムにおける処理の概要を示す処理概略図である。

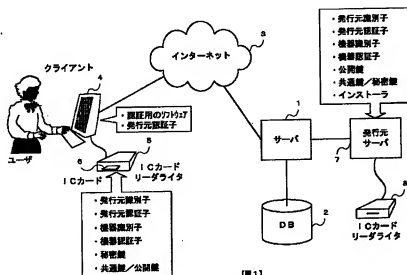
【図3】サーバ1における処理の流れを示すフローチャートである。

【図4】ICカード6における処理の流れを示すフローチャートである。

【符号の説明】

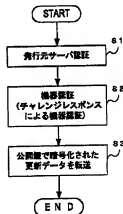
1…サーバ、 2…DB、 3…インターネット、 4…クライアント、 5…ICカードリーダライタ、 6…ICカード、 7…発行元サーバ、 8…ICカードリーダライタ

【図1】



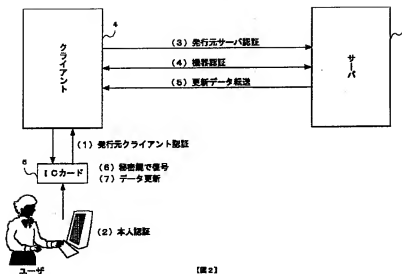
【図1】

【図3】



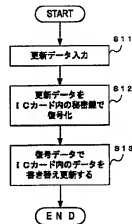
【図3】

【図2】



【図2】

【図4】



【図4】

## 【手続補正書】

【提出日】平成15年4月7日(2003.4.7)

## 【手続補正1】

【補正対象書類名】明細書

【補正対象項目名】請求項3

【補正方法】変更

【補正内容】

【請求項3】 機器認証に用いる秘密鍵を記憶する装置には、共通鍵又は公開鍵で暗号化された発行元認証子が記憶され、サーバは前記共通鍵又は前記公開鍵に対応する秘密鍵を用い、前記装置からの暗号化された発行元認証子を当該共通鍵又は当該秘密鍵で復号して発行元識別子を取得し、当該取得した発行元識別子と記憶する発行元識別子とを比較照合して発行元サーバ認証を行うことを特徴とする請求項1又は2記載のデータ更新方法。

## 【手続補正2】

【補正対象書類名】明細書

【補正対象項目名】請求項8

【補正方法】変更

【補正内容】

【請求項8】 サーバは、乱数を発生させ、当該乱数をクライアントに送信すると共に、前記クライアントから受信した暗号化された乱数を受信した機器識別子に対応する公開鍵で復号し、当該復号された乱数と前記発生させた乱数を比較照合して機器認証を行うサーバであり、前記クライアントは、前記サーバから受信した乱数を装置に出力すると共に、前記装置から入力された暗号化された乱数及び機器識別子を前記サーバに送信するクライアントであり、

前記装置は、前記クライアントから入力された乱数を、記憶する秘密鍵で暗号化し、記憶する機器識別子と前記暗号化された乱数を前記クライアントに出力する装置であることを特徴とする請求項6又は7記載のデータ更新システム。

## 【手続補正3】

【補正対象書類名】明細書

【補正対象項目名】請求項9

【補正方法】変更

【補正内容】

【請求項9】 サーバは、乱数と、機器識別子を暗号化するための共通鍵をクライアントに送信し、前記クライアントから受信した暗号化された機器識別子を前記共通鍵で復号し、当該復号された機器識別子に対応する公開鍵で暗号化された乱数を復号し、当該復号された乱数と前記発生させた乱数を比較照合して機器認証を行うサーバであり、

前記クライアントは、前記サーバから受信した乱数及び共通鍵を装置に出力すると共に、前記装置から入力された暗号化された乱数及び暗号化された機器識別子を前記サーバに送信するクライアントであり、

前記装置は、前記クライアントから入力された乱数を、記憶する秘密鍵で暗号化し、記憶する機器識別子を前記共通鍵で暗号化し、前記暗号化された乱数及び前記暗号化された機器識別子を前記クライアントに出力する装置であることを特徴とする請求項8記載のデータ更新システム。

## 【手続補正4】

【補正対象書類名】明細書

【補正対象項目名】請求項 12

【補正方法】変更

【補正内容】

【請求項 12】 装置は、発行元認証に用いる共通鍵又は公開鍵を記憶し、当該共通鍵又は公開鍵で暗号化された発行元認証子をクライアントに出力する装置であり、前記クライアントは、前記暗号化された発行元認証子をサーバに送信するクライアントであり、前記サーバは、発行元認証に用いる共通鍵又は秘密鍵を記憶し、前記クライアントから受信した暗号化された発行元認証子を当該記憶する共通鍵又は秘密鍵で復号して発行元識別子を取得し、当該取得した発行元識別子と記憶する発行元識別子とを比較照合して発行元サーバ認証を行うサーバであることを特徴とする請求項 8乃至 11のいずれかに記載のデータ更新システム。

【手続補正 5】

【補正対象書類名】明細書

【補正対象項目名】0002

【補正方法】変更

【補正内容】

【0002】

【従来の技術】従来、ICカード（スマートカード）や、その他取り外し可能な本人認証の機能を備えた装置に記憶された重要なデータ、例えば、ネットワークパスワード、電子証明書、シングルサインオンするための情報を追加する場合や、ダイヤルアップ情報、ICカード／スマートカードや指紋照合トークン情報、有効期限等の重要な情報を更新する場合には、当該ICカードを一旦回収してデータの書き換えを行って本人に戻すか、そのカードを無効にして更新データが書き込まれた新規のカードを本人に発行するかのいずれかの方法が採用されている。

【手続補正 6】

【補正対象書類名】明細書

【補正対象項目名】0005

【補正方法】変更

【補正内容】

【0005】本発明は上記実情に鑑みて為されたものであり、装置を間違えず特定し、ネットワークを介して記録媒体のデータの新規登録や追加登録を含む更新を自動で又は処理を起動して行うことができるデータ更新方法及びデータ更新システムを提供することを目的とする。

【手続補正 7】

【補正対象書類名】明細書

【補正対象項目名】0011

【補正方法】変更

【補正内容】

【0011】

【発明の実施の形態】本発明の実施の形態について図面を参照しながら説明する。本発明の実施の形態に係るデータ更新システムは、本人認証、発行元認証、機器認証の各認証が為され、機器認証子に対応する公開鍵で暗号化された更新データをサーバがクライアントに送信すると、ICカードが当該暗号化された更新データをICカード内の機器認証子に対応する秘密鍵で復号化し、その復号した更新データでICカード内の書き換えを行うものである。これにより、ICカードを回収することなく、重要データの秘匿性を保持しつつネットワークを介してICカード内の重要データの更新（新規登録又は追加登録を含む）を自動で又は処理を起動して行うことができるものである。

【手続補正 8】

【補正対象書類名】明細書

【補正対象項目名】0029

【補正方法】変更

【補正内容】

【0029】ICカード6は、CPU（Central Processing Unit）を備えて独立して処理を行うことができるものであり、本人認証を行う生体データ、PINデータと、発行元認証を行うための発行元識別子、発行元認証子、共通鍵／公開鍵と、機器認証を行うための機器識別子、秘密鍵とを記憶している。ここで、各データは、ICカード6を無理にこじ開けた場合に、消滅する耐タンパー性を備えている。

【手続補正 9】

【補正対象書類名】明細書

【補正対象項目名】0039

【補正方法】変更

【補正内容】

【0039】本人認証が適正であれば、次に、ICカード6は、発行元認証子をクライアント4からサーバ1に送信してサーバ1での発行元サーバ認証（3）を行う（S1）。発行元サーバ認証は、ICカード6から出力された発行元認証子をサーバ1が受信し、DB2に記憶する復号のための共通鍵／秘密鍵を用いて復号化し、復号された発行元識別子を取得して、DB2に記憶する発行元識別子と比較照合する。比較照合の結果、一致すれば発行元サーバ認証が成功したとして、次に機器認証（4）を行う。